

66/29  
66/29  
U.S. PTO  
F571  
66/29/80

Please type a plus sign (+) inside this box **[+]**

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

7525-06-5 pro  
09/386589  
08/29/99

## UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 42390.P7574

Total Pages 2

First Named Inventor or Application Identifier Gary L. Graunke

Express Mail Label No. EL 414969073 US

ADDRESS TO: **Assistant Commissioner for Patents**  
**Box Patent Application**  
**Washington, D. C. 20231**

### APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1.  Fee Transmittal Form  
(Submit an original, and a duplicate for fee processing)
2.  Specification (Total Pages 25)  
(preferred arrangement set forth below)
  - Descriptive Title of the Invention
  - Cross References to Related Applications
  - Statement Regarding Fed sponsored R & D
  - Reference to Microfiche Appendix
  - Background of the Invention
  - Brief Summary of the Invention
  - Brief Description of the Drawings (if filed)
  - Detailed Description
  - Claims
  - Abstract of the Disclosure
3.  Drawings(s) (35 USC 113) (Total Sheets 3)
4.  Oath or Declaration (Total Pages 4)
  - a.  Newly Executed (Original or Copy)
  - b.  Copy from a Prior Application (37 CFR 1.63(d))  
(for Continuation/Divisional with Box 17 completed) (Note Box 5 below)
  - i.  **DELETIONS OF INVENTOR(S)** Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5.  Incorporation By Reference (useable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6.  Microfiche Computer Program (Appendix)

7.  Nucleotide and/or Amino Acid Sequence Submission  
(if applicable, all necessary)

- a.  Computer Readable Copy
- b.  Paper Copy (identical to computer copy)
- c.  Statement verifying identity of above copies

**ACCOMPANYING APPLICATION PARTS**

8.  Assignment Papers (cover sheet & documents(s))

9.  a. 37 CFR 3.73(b) Statement (where there is an assignee)

b. Power of Attorney

10.  English Translation Document (if applicable)

11.  a. Information Disclosure Statement (IDS)/PTO-1449

b. Copies of IDS Citations

12.  Preliminary Amendment

13.  Return Receipt Postcard (MPEP 503) (Should be specifically itemized)

14.  a. Small Entity Statement(s)

b. Statement filed in prior application, Status still proper and desired

15.  Certified Copy of Priority Document(s) (if foreign priority is claimed)

16.  Other: Separate sheet with Certificate of Mailing, attorney signature and  
registration number and copy of return postcard

17. If a **CONTINUING APPLICATION**, check appropriate box and supply the requisite information:

Continuation  Divisional  Continuation-in-part (CIP)

of prior application No: \_\_\_\_\_

18. **Correspondence Address**

Customer Number or Bar Code Label \_\_\_\_\_ (Insert Customer No. or Attach Bar Code Label here)

or

Correspondence Address Below

NAME Aloysius T. C. AuYeung

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard

Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (503) 684-6200 FAX (503) 684-3245

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

**A Stream Cipher Having  
A Shuffle Network Combiner Function**

"Express Mail" mailing label number EL 414969073 US

Date of Deposit AUGUST 29, 1999

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Address" service on the date indicated above and that this paper or fee has been delivered to the Assistant Commissioner for Patents, Washington, D.C. 20231

Judith G. Nwonye 8/29/99  
Signature Date

Inventor(s): **Gary L. Graunke  
David A. Lee  
Robert W. Faber**

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP  
12400 Wilshire Boulevard, 7th Floor  
Los Angeles, California 90025  
(503) 684-6200

"Express Mail" label number EL 41469073 US

## **A Stream Cipher Having A Shuffle Network Combiner Function**

### **BACKGROUND OF THE INVENTION**

5    1.    **Field of the Invention**

The present invention relates to the field of cryptography. More specifically, the present invention relates to the robustness of stream ciphers.

10    2.    **Background Information**

10    Cryptographic ciphers can be broadly divided into block ciphers and stream ciphers. Block ciphers cipher a block of plain text into ciphered text by applying multiple successive rounds of transformation to the plain text, using a cipher key. An example of a block cipher is the well known DES cipher. Stream ciphers cipher a stream of plain data into ciphered data by combining the stream of plain data with a pseudo random sequence dynamically generated using a cipher key. An example of a stream cipher is the well known XPF/KPD cipher.

15    Most stream ciphers employ one or more linear feedback shift registers (LFSR). In various applications, it is desirable to employ multiple LFSRs to increase the robustness of a stream cipher. However, employment of multiple LFSRs requires employment of a combiner function to recombine the multiple data bits output by the LFSRs. Most combiner functions known in the art are inefficient in their real estate requirement for hardware implementations. Thus, a robust stream cipher with a more efficient combiner function is desired.

25

## SUMMARY OF THE INVENTION

A stream cipher is provided with one or more data bit generators to generate a first, second and third set of data bits. The stream cipher is further provided with a 5 combiner function having a network of shuffle units to combine the third set of data bits, using the first and second sets of data bits as input data bits and control signals respectively of the network of shuffle units.

## BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references 5 denote similar elements, and in which:

**Figure 1** illustrates an overview of the combined block/stream cipher of the present invention, in accordance with one embodiment;

**Figure 2** illustrates the block key section of **Fig. 1** in further detail, in accordance with one embodiment;

10 **Figure 3** illustrates the block data section of **Fig. 1** in further detail, in accordance with one embodiment;

**Figures 4a-4c** illustrate the stream data section of **Fig. 1** in further detail, in accordance with one embodiment; and

15 **Figure 5** illustrates a bit-wise view of the mapping section of **Fig. 1** in further detail, in accordance with one embodiment.

## DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention.

However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating the combined block/stream cipher of the present invention, in accordance with one embodiment, is shown. As illustrated, combined block/stream cipher **110** includes block key section **502**, data section **504**, stream key section **506**, and mapping section **508**, coupled to one another. Block key section **502** and data section **504** are employed in both the block mode as well as the stream mode of operation, whereas stream key section **506** and mapping section **508** are employed only in the stream mode of operation.

Briefly, in block mode, block key section **502** is provided with a block cipher key, such as an authentication key  $K_m$  or a session key  $K_s$  of a video content protection application; whereas data section **504** is provided with the plain text, such

as a basis random number An or a derived random number Mi-1 of a video content protection application. “Rekeying enable” signal is set to a “disabled” state, operatively de-coupling block key section **502** from stream key section **506** during the block mode of operation.

5 [A video content protection application that uses Km, Kx, An and Mi is described in copending U.S. Patent Applications, serial numbers, <to be inserted>, filed contemporaneously, both entitled “Digital Video Content Transmission Ciphering/Deciphering Method and Apparatus”, having common assignee and inventorship with the present application.]

10 During each clock cycle, the block cipher key as well as the plain text are transformed. The block cipher key is independently transformed, whereas transformation of the plain text is dependent on the transformation being performed on the block cipher key. After a desired number of clock cycles, the provided plain text is transformed into ciphered text. For the video content protection method 15 disclosed in above mentioned co-pending applications, when block key section **502** is provided with Km and data section **504** is provided with the An, ciphered An is read out and used as the session key Ks. When block key section **502** is provided with Ks and data section **504** is provided with the Mi-1, ciphered Mi-1 is read out and used as the frame key Ki.

20 To decipher the ciphered plain text, block key section **502** and data section **504** are used in like manner as described above to generate the intermediate “keys”, which are stored away (in storage locations not shown). The stored intermediate “keys” are then applied to the ciphered text in reversed order, resulting in the deciphering of the ciphered text back into the original plain text. Another approach 25 to deciphering the ciphered text will be described after block key section **502** and

data section **504** have been further described in accordance with one embodiment each, referencing **Figs. 2-3**.

In stream mode, stream key section **506** is provided with a stream cipher key, such as a session key  $K_s$  or a frame key  $K_i$  of a video content protection application.

5 Block key section **502** and data section **504** are provided with random numbers, such as a session/frame keys  $K_s/K_i$  and a derived random numbers  $M_{i-1}$  of a video content protection application. “Rekeying enable” signal is set to an “enabled” state, operatively coupling block key section **502** to stream key section **506**. Periodically, at predetermined intervals, such as the horizontal blanking intervals of a video

10 frame, stream key section **506** is used to generate one or more data bits to dynamically modify the then current state of the random number stored in block data section **502**. During each clock cycle, in between the predetermined intervals, both random numbers stored in block key section **502** and data section **504** are transformed. The random number provided to block key section **502** is

15 independently transformed, whereas transformation of the random number provided to data section **504** is dependent on the transformation being performed in block key section **502**. Mapping block **506** retrieves a subset each, of the newly transformed states of the two random numbers, and reduces them to generate one bit of the pseudo random bit sequence. Thus, in a desired number of clock cycles, a pseudo

20 random bit sequence of a desired length is generated.

For the illustrated embodiment, by virtue of the employment of the “rekeying enable” signal, stream key section **506** may be left operating even during the block mode, as its outputs are effectively discarded by the “rekeying enable” signal (set in a “disabled” state).

**Figure 2** illustrates the block key section of **Fig. 1** in further detail, in accordance with one embodiment. As illustrated, block key section **502** includes registers **602a-602c**, substitution boxes **604**, and linear transformation unit **606**. In block mode, registers **602a-602c** are collectively initialized to a block cipher key, e.g.

5 the earlier mentioned authentication key  $K_m$  or session key  $K_s$ . In stream mode, registers **602a-602c** are collectively initialized to a random number, e.g. the earlier mentioned session key  $K_s$  or frame key  $K_i$ . Each round, substitution boxes **604** and linear transformation unit **606** modify the content of registers **602a-602c**. More specifically, substitution boxes **604** receive the content of register **602a**, modify it, 10 and then store the substituted content into register **602c**. Similarly, linear transformation unit **606** receives the content of registers **602b** and **602c**, linearly transforms them, and then correspondingly stores the linearly transformed content into registers **602a** and **602b**.

Substitution boxes **604** and linear transformation unit **606** may be 15 implemented in a variety of ways in accordance with well known cryptographic principles. One specific implementation is given in more detail below after the description of **Fig. 3**.

**Figure 3** illustrates the block data section of **Fig. 1** in further detail, in accordance with one embodiment. For the illustrated embodiment, data section **504** 20 is similarly constituted as block key section **502**, except linear transformation unit **706** also takes into consideration the content of register **602b**, when transforming the contents of registers **702b-702c**. In block mode, registers **702a-702c** are collectively initialized with the target plain text, e.g. earlier described random number  $A_n$  or derived random number  $M_{i-1}$ . In stream mode, registers **702a-702c** are 25 collectively initialized with a random number. Each round, substitution boxes **704**

and linear transformation unit **706** modify the content of registers **702a-702c** as described earlier for block key section **502** except for the differences noted above.

Again, substitution boxes **604** and linear transformation unit **606** may be implemented in a variety of ways in accordance with well known cryptographic

5 principles.

In one implementation for the above described embodiment, each register **602a**, **602b**, **602c**, **702a**, **702b**, **702c** is 28-bit wide. [Whenever registers **602a-602c** or **702a-702cb** collectively initialized with a key value or random number less than 84 bits, the less than 84-bit number is initialized to the lower order bit positions with

10 the higher order bit positions zero filled.] Additionally, each set of substitution boxes **604** or **704** are constituted with seven 4 input by 4 output substitution boxes. Each

linear transformation unit **606** or **706** produces 56 output values by combining outputs from eight diffusion networks (each producing seven outputs). More specifically, the operation of substitution boxes **604/704** and linear transformation

15 unit **606/706** are specified by the four tables to follow. For substitution boxes **604/704**, the  $I$ th input to box  $J$  is bit  $I*7+J$  of register **602a/702a**, and output  $I$  of box  $J$  goes to bit  $I*7+j$  of register **602c/702c**. [Bit 0 is the least significant bit.] For each diffusion network (linear transformation unit **606** as well as **706**), the inputs are generally labeled  $I0-I6$  and the outputs are labeled  $O0-O6$ . The extra inputs for

20 each diffusion network of the linear transformation unit **706** is labeled  $K0-K6$ .

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SK0	8	14	5	9	3	0	12	6	1	11	15	2	4	7	10	13
SK1	1	6	4	15	8	3	11	5	10	0	9	12	7	13	14	2
SK2	13	11	8	6	7	4	2	15	1	12	14	0	10	3	9	5
SK3	0	14	11	7	12	3	2	13	15	4	8	1	9	10	5	6
SK4	12	7	15	8	11	14	1	4	6	10	3	5	0	9	13	2
SK5	1	12	7	2	8	3	4	14	11	5	0	15	13	6	10	9
SK6	10	7	6	1	0	14	3	13	12	9	11	2	15	5	4	8
SB0	12	9	3	0	11	5	13	6	2	4	14	7	8	15	1	10
SB1	3	8	14	1	5	2	11	13	10	4	9	7	6	15	12	0
SB2	7	4	1	10	11	13	14	3	12	15	6	0	2	8	9	5
SB3	6	3	1	4	10	12	15	2	5	14	11	8	9	7	0	13
SB4	3	6	15	12	4	1	9	2	5	8	10	7	11	13	0	14
SB5	11	14	6	8	5	2	12	7	1	4	15	3	10	13	9	0
SB6	1	11	7	4	2	5	12	9	13	6	8	15	14	0	3	10

Table I – Substitution performed by each of the seven constituting substitution boxes of substitution boxes **604/704**.

5

Diffusion Network Logic Function						
<b>O<sub>0</sub></b>	$K_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$					
<b>O<sub>1</sub></b>	$K_1 \oplus I_0 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$					
<b>O<sub>2</sub></b>	$K_2 \oplus I_0 \oplus I_1 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$					
<b>O<sub>3</sub></b>	$K_3 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_4 \oplus I_5 \oplus I_6$					
<b>O<sub>4</sub></b>	$K_4 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_5 \oplus I_6$					
<b>O<sub>5</sub></b>	$K_5 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_6$					
<b>O<sub>6</sub></b>	$K_6 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$					

Table II – Diffusion networks for linear transformation unit **606/706** (continued in Tables III & IV).

	<b>K1</b>	<b>K2</b>	<b>K3</b>	<b>K4</b>	<b>K5</b>	<b>K6</b>	<b>K7</b>	<b>K8</b>
<b>I<sub>0</sub></b>	Kz0	Ky0	Ky4	Ky8	Ky12	Ky16	Ky20	Ky24
<b>I<sub>1</sub></b>	Kz1	Ky1	Ky5	Ky9	Ky13	Ky17	Ky21	Ky25
<b>I<sub>2</sub></b>	Kz2	Ky2	Ky6	Ky10	Ky14	Ky18	Ky22	Ky26
<b>I<sub>3</sub></b>	Kz3	Ky3	Ky7	Ky11	Ky15	Ky19	Ky23	Ky27
<b>I<sub>4</sub></b>	Kz4	Kz7	Kz10	Kz13	Kz16	Kz19	Kz22	Kz25
<b>I<sub>5</sub></b>	Kz5	Kz8	Kz11	Kz14	Kz17	Kz20	Kz23	Kz26
<b>I<sub>6</sub></b>	Kz6	Kz9	Kz12	Kz15	Kz18	Kz21	Kz24	Kz27
<b>O<sub>0</sub></b>	Kx0	Ky0	Ky1	Ky2	Ky3	Kx7	Kx8	Kx9
<b>O<sub>1</sub></b>	Kx1	Ky4	Ky5	Ky6	Ky7	Kx10	Kx11	Kx12
<b>O<sub>2</sub></b>	Kx2	Ky8	Ky9	Ky10	Ky11	Kx13	Kx14	Kx15
<b>O<sub>3</sub></b>	Kx3	Ky12	Ky13	Ky14	Ky15	Kx16	Kx17	Kx18
<b>O<sub>4</sub></b>	Kx4	Ky16	Ky17	Ky18	Ky19	Kx19	Kx20	Kx21
<b>O<sub>5</sub></b>	Kx5	Ky20	Ky21	Ky22	Ky23	Kx22	Kx23	Kx24
<b>O<sub>6</sub></b>	Kx6	Ky24	Ky25	Ky26	Ky27	Kx25	Kx26	Kx27

Table III – Diffusion networks for linear transformation unit **606/706** (continued in Table IV).

	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
<b>I<sub>0</sub></b>	Bz0	By0	By4	By8	By12	By16	By20	By24
<b>I<sub>1</sub></b>	Bz1	By1	By5	By9	By13	By17	By21	By25
<b>I<sub>2</sub></b>	Bz2	By2	By6	By10	By14	By18	By22	By26
<b>I<sub>3</sub></b>	Bz3	By3	By7	By11	By15	By19	By23	By27
<b>I<sub>4</sub></b>	Bz4	Bz7	Bz10	Bz13	Bz16	Bz19	Bz22	Bz25
<b>I<sub>5</sub></b>	Bz5	Bz8	Bz11	Bz14	Bz17	Bz20	Bz23	Bz26
<b>I<sub>6</sub></b>	Bz6	Bz9	Bz12	Bz15	Bz18	Bz21	Bz24	Bz27
<b>K<sub>0</sub></b>	Ky0	—	—	—	—	Ky7	Ky14	Ky21
<b>K<sub>1</sub></b>	Ky1	—	—	—	—	Ky8	Ky15	Ky22
<b>K<sub>2</sub></b>	Ky2	—	—	—	—	Ky9	Ky16	Ky23
<b>K<sub>3</sub></b>	Ky3	—	—	—	—	Ky10	Ky17	Ky24
<b>K<sub>4</sub></b>	Ky4	—	—	—	—	Ky11	Ky18	Ky25
<b>K<sub>5</sub></b>	Ky5	—	—	—	—	Ky12	Ky19	Ky26
<b>K<sub>6</sub></b>	Ky6	—	—	—	—	Ky13	Ky20	Ky27
<b>O<sub>0</sub></b>	Bx0	By0	By1	By2	By3	Bx7	Bx8	Bx9
<b>O<sub>1</sub></b>	Bx1	By4	By5	By6	By7	Bx10	Bx11	Bx12
<b>O<sub>2</sub></b>	Bx2	By8	By9	By10	By11	Bx13	Bx14	Bx15
<b>O<sub>3</sub></b>	Bx3	By12	By13	By14	By15	Bx16	Bx17	Bx18
<b>O<sub>4</sub></b>	Bx4	By16	By17	By18	By19	Bx19	Bx20	Bx21
<b>O<sub>5</sub></b>	Bx5	By20	By21	By22	By23	Bx22	Bx23	Bx24
<b>O<sub>6</sub></b>	Bx6	By24	By25	By26	By27	Bx25	Bx26	Bx27

Table IV – Diffusion networks for linear transformation unit **606/706** (continued from Table III).

5 Referring now back to **Fig. 5**, recall that a ciphered text may be deciphered by generating the intermediate “keys” and applying them backward. Alternatively, for an embodiment where either the inverse of substitution boxes **604/704** and linear transformation units **606/706** are included or they may be dynamically reconfigured to operate in an inverse manner, the ciphered text may be deciphered as follows.

10 First, the cipher key used to cipher the plain text is loaded into block key section **502**, and block key section **502** is advanced by R-1 rounds, i.e. one round short of

the number of rounds (R) applied to cipher the plain text. After the initial R-1 rounds, the ciphered text is loaded into data section **504**, and both sections, block key section **502** and data section **504**, are operated “backward”, i.e. with substitution boxes **604/704** and linear transformation units **606/706** applying the inverse

5 substitutions and linear transformations respectively.

**Figures 4a-4c** illustrate the stream key section of **Fig. 1** in further detail, in accordance with one embodiment. As illustrated in **Fig. 4a**, stream key section **506** includes a number of linear feedback shift registers (LFSRs) **802** and combiner function **804**, coupled to each other as shown. LFSRs **802** are collectively initialized 10 with a stream cipher key, e.g. earlier described frame key  $K_i$ . During operation, the stream cipher key is successively shifted through LFSRs **802**. Selective outputs are taken from LFSRs **802**, and combiner function **804** is used to combine the selective outputs. In stream mode (under which, rekeying is enabled), the combined result is used to dynamically modify a then current state of a block cipher key in block key 15 section **502**.

For the illustrated embodiment, four LFSRs of different lengths are employed. Three sets of outputs are taken from the four LFSRs. The polynomials represented by the LFSR and the bit positions of the three sets of LFSR outputs are given by the table to follows:

20

LFSR	Polynomial	Combining Function		
		0	1	2
3	$X^{17} + X^{15} + X^{11} + X^5 + 1$	6	12	17
2	$X^{16} + X^{15} + X^{12} + X^8 + X^7 + X^5 + 1$	6	10	16
1	$X^{14} + X^{11} + X^{10} + X^7 + X^6 + X^4 + 1$	5	9	14
0	$X^{13} + X^{11} + X^9 + X^5 + 1$	4	8	13

Table V – Polynomials of the LFSR and tap positions.

The combined result is generated from the third set of LFSR outputs, using

5 the first and second set of LFSR outputs as data and control inputs respectively to combiner function 802. The third set of LFSR outputs are combined into a single bit. In stream mode (under which, rekeying is enabled), the combined single bit is then used to dynamically modify a predetermined bit of a then current state of a block cipher key in block key section 502.

10 Fig. 4b illustrates combiner function 804 in further detail, in accordance with one embodiment. As illustrated, combiner function 804 includes shuffle network 806 and XOR 808a-808b, serially coupled to each other and LFSRs 802 as shown. For the illustrated embodiment, shuffle network 806 includes four binary shuffle units 810a-810d serially coupled to each other, with first and last binary shuffle units 810a and 810d coupled to XOR 808a and 808b respectively. XOR 808a takes the first group of LFSR outputs and combined them as a single bit input for shuffle network 806. Binary shuffle units 810a-810d serially propagate and shuffle the output of XOR 808a. The second group of LFSR outputs are used to control the shuffling at corresponding ones of binary shuffle units 810a-810d. XOR 808b combines the 15 third set of LFSR outputs with the output of last binary shuffle unit 810d.

15

20

**Fig. 4c** illustrates one binary shuffle unit **810\*** (where \* is one of a-d) in further detail, in accordance with one embodiment. Each binary shuffle unit **810\*** includes two flip-flops **812a** and **812b**, and a number of selectors **814a-814c**, coupled to each other as shown. Flip-flops **812a** and **812b** are used to store two state values (A, B). Each selector **814a**, **814b** or **814c** receives a corresponding one of the second group of LFSR outputs as its control signal. Selector **814a-814b** also each receives the output of XOR **808a** or an immediately preceding binary shuffle unit **810\*** as input. Selector **814a-814b** are coupled to flip-flops **812a-812b** to output one of the two stored state values and to shuffle as well as modify the stored values in accordance with the state of the select signal. More specifically, for the illustrated embodiment, if the stored state values are (A, B), and the input and select values are (D, S), binary shuffle unit **810\*** outputs A, and stores (B, D) if the value of S is "0". Binary shuffle unit **810\*** outputs B, and stores (D, A) if the value of S is "1".

Referring now to back to **Figure 1**, as illustrated and described earlier, mapping function **508** generates the pseudo random bit sequence based on the contents of selected registers of block key section **502** and data section **504**. In one embodiment, where block key section **502** and data section **504** are implemented in accordance with the respective embodiments illustrated in **Fig. 2-3**, mapping function **508** generates the pseudo random bit sequence at 24-bit per clock based on the contents of registers (Ky and Kz) **602b-602c** and (By and Bz) **702b-702c**. More specifically, each of the 24 bits is generated by performing the XOR operation on nine terms in accordance with the following formula:

$$(B0 \bullet K0) \oplus (B1 \bullet K1) \oplus (B2 \bullet K2) \oplus (B3 \bullet K3) \oplus (B4 \bullet K4) \oplus (B5 \bullet K5) \oplus (B6 \bullet K6) \oplus$$

25       $B7 \oplus K7$

Where “ $\oplus$ ” represents a logical XOR function, “ $\bullet$ ” represents a logical AND function, and the input values B and K for the 24 output bits are

Input Origin Output bit	B0 Bz	B1 Bz	B2 Bz	B3 Bz	B4 Bz	B5 Bz	B6 Bz	B7 By	K0 Kz	K1 Kz	K2 Kz	K3 Kz	K4 Kz	K5 Kz	K6 Kz	K7 Ky
0	14	23	7	27	3	18	8	20	12	24	0	9	16	7	20	13
1	20	26	6	15	8	19	0	10	26	18	1	11	6	20	12	19
2	7	20	2	10	19	14	26	17	1	22	8	13	7	16	25	3
3	22	12	6	17	3	10	27	4	24	2	9	5	14	18	21	15
4	22	24	14	18	7	1	9	21	19	24	20	8	13	6	3	5
5	12	1	16	5	10	24	20	14	27	2	8	16	15	22	4	21
6	5	3	27	8	17	15	21	12	14	23	16	10	27	1	7	17
7	9	20	1	16	5	25	12	6	9	13	22	17	1	24	5	11
8	23	25	11	13	17	1	6	22	25	21	18	15	6	11	1	10
9	4	0	22	17	25	10	15	18	0	20	26	19	4	15	9	27
10	23	25	9	2	13	16	4	8	2	11	27	19	14	22	4	7
11	3	6	20	12	25	19	10	27	24	3	14	6	23	17	10	1
12	26	1	18	21	14	4	10	0	17	7	26	0	23	11	14	8
13	2	11	4	21	15	24	18	9	5	16	12	2	26	23	11	6
14	22	24	3	19	11	4	13	5	22	0	18	8	25	5	15	2
15	12	0	27	11	22	5	16	1	10	3	15	19	21	27	6	18
16	24	20	2	7	15	18	8	3	12	20	5	19	1	27	8	23
17	12	16	8	24	7	2	21	23	17	2	11	14	7	25	22	16
18	19	3	22	9	13	6	25	7	4	10	2	17	21	24	13	22
19	11	17	13	26	4	21	2	16	3	4	13	26	18	23	9	25
20	17	23	26	14	5	11	0	15	26	3	9	19	21	12	6	0
21	9	14	23	16	27	0	6	24	18	21	3	27	4	10	15	26
22	7	21	8	13	1	26	19	25	25	0	12	10	7	17	23	9
23	27	15	23	5	0	9	18	11	8	0	25	20	16	5	13	12

5 Accordingly, a novel dual use block or stream cipher has been described.

### Epilogue

From the foregoing description, those skilled in the art will recognize that many other variations of the present invention are possible. In particular, while the 10 present invention has been described with the illustrated embodiments, non-LFSR based stream key section, more or less block key registers, larger or smaller block

key registers, more or less substitution units, including alternative substitution patterns, as well as different linear transformation units may be employed. Thus, the present invention is not limited by the details described, instead, the present invention can be practiced with modifications and alterations within the spirit and

## 5 scope of the appended claims.

CLAIMS

What is claimed is:

- 1 1. An apparatus comprising:
  - 2 at least one data bit generator to generate a first, second and third plurality of
  - 3 data bits; and
  - 4 a combiner function, coupled to the at least one data bit generator, including
  - 5 a network of shuffle units, to combine the third plurality of data bits, using the first
  - 6 and second plurality of data bits as first input data bits and control signals
  - 7 respectively of the network of shuffle units.
- 1 2. The apparatus of claim 1, wherein at least one of the shuffle units comprises
- 2 a first and a second flip-flop to store a first and a second state value, and a plurality
- 3 of selectors coupled to the first and second flip-flops in a topological manner to
- 4 control selective output of one of the first and second state values based on a
- 5 corresponding one of said second plurality of data bits.
- 1 3. The apparatus of claim 2, wherein said plurality of selectors are coupled to
- 2 said first and second flip-flops of the shuffle unit in a topological manner that results
- 3 in the first state value of the shuffle unit being output when the corresponding one of
- 4 said second plurality of data bits is in a first state, and the second state value of the
- 5 shuffle unit being output when the corresponding one of said second plurality of data
- 6 bits is in a second state.

1 4. The apparatus of claim 2, wherein said plurality of the selectors are further  
2 coupled to said first and second flip-flops of the shuffle unit to control selective  
3 modification of the first and second state values stored in said first and second flip-  
4 flops of the shuffle unit based on the same corresponding one of said second  
5 plurality of data bits.

1 5. The apparatus of claim 4, wherein said plurality of selectors are coupled to  
2 said first and second flip-flops of the shuffle unit in a topological manner that results  
3 in the first state value being ~~output~~ and the first and second flip-flops of the shuffle  
4 unit to store said second state value and a second input data bit respectively when  
5 the corresponding one of said second plurality of data bits is in a first state, and the  
6 second state value being ~~output~~ and the first and second flip-flops of the shuffle unit  
7 to store the second input data bit and said first state value respectively when the  
8 corresponding one of said second plurality of data bits is in a second state.

1 6. The apparatus of claim 5, wherein the second input value is a selected one of  
2 an output data bit of an ~~immediately~~ preceding shuffle unit and an output data bit  
3 generated from said first plurality of data bits.

1 7. The apparatus of claim 1, wherein at least one of the shuffle units comprises  
2 a first and a second flip-flop to store a first and a second state value, and a plurality  
3 of selectors coupled to the first and second flip-flops to control modification of the  
4 first and second state values based on a corresponding one of said second plurality  
5 of data bits.

**PRINT OF DRAWINGS  
AS ORIGINALLY FILED**

Attorney Docket Ref: 42390.P7574

1 8. The apparatus of claim 7, wherein said plurality of selectors are coupled to  
2 the first and second flip-flops in a topological manner that results in the first and  
3 second flip-flops of the ~~shuffle~~ unit to store said second state value and a second  
4 input data bit respectively when the corresponding one of said second plurality of  
5 data bits is in a first state, and the first and second flip-flops of the ~~shuffle~~ unit to  
6 store the second input data bit and said first state value respectively when the  
7 corresponding one of said second plurality of data bits is in a second state.

1 9. The apparatus of claim 8, wherein the ~~shuffle~~ units are serially coupled to  
2 each other with a first of the ~~shuffle~~ unit serially coupled to the first XOR gate, and  
3 said second input data bit is a selected one of an output bit of an immediately  
4 preceding ~~shuffle~~ unit and an output bit generated from the first plurality of data bits.

1 10. The apparatus of claim 1, wherein the combiner function further comprises an  
2 exclusive-OR gate to combine the first plurality of data bits for the network of ~~shuffle~~  
3 units.

1 11. The apparatus of claim 1, wherein the combiner function further comprises an  
2 exclusive-OR gate to combine the third plurality of data bits using an output bit of the  
3 network of ~~shuffle~~ units.

1 12. The apparatus of claim 11, wherein the apparatus further comprises a  
2 register coupled to the XOR gate to store a cipher key and allow the stored cipher  
3 key to be periodically modified by the output of the exclusive-OR gate.

1 13. The apparatus of claim 12, wherein the apparatus further comprises a  
2 function block coupled to the register to successively transform the modified cipher  
3 key, and a mapping block coupled to the register to generate a pseudo random bit  
4 sequence based on the successive transformed states of the modified random  
5 number.

1 14. The apparatus of claim 1, wherein the at least one data bit generator  
2 comprises a plurality of LFSRs to generate said first, second, and third plurality of  
3 data bits.

1 15. The apparatus of claim 1, wherein the apparatus is a stream cipher.

1 14. An apparatus comprising:  
2 a first XOR gate to receive a first plurality of data bits and combine them into  
3 a second data bit;  
4 a network of shuffle units, coupled to the first XOR gate, to output a third data  
5 bit by shuffling and propagating the second data bit through the network of shuffle  
6 units under the control of a four plurality of data bits; and  
7 a second XOR gate coupled to the network of shuffle units to combine a fifth  
8 plurality of data bits using the third data bit.

1 15. The apparatus of claim 14, wherein at least one of the shuffle units comprises  
2 a first and a second flip-flop to store a first and a second state value, and a plurality  
3 of selectors coupled to the first and second flip-flops to control selective output of  
4 one of the first and second state values based on a corresponding one of said fourth  
5 plurality of data bits.

1 16. The apparatus of claim 15, wherein said plurality of selectors are coupled to  
2 the first and second flip-flops of the shuffle unit in a topological manner that results  
3 in the first state value of the shuffle unit being output when the corresponding one of  
4 said fourth plurality of data bits is in a first state, and the second state value of the  
5 shuffle unit being output when the corresponding one of said fourth plurality of data  
6 bits is in a second state.

1 17. The apparatus of claim 16, wherein said plurality of the selectors are further  
2 coupled to the first and second flip-flops to control selective modification of the first  
3 and second state values stored in the first and second flip-flops of the shuffle unit  
4 based on the same corresponding one of said fourth plurality of data bits.

1 18. The apparatus of claim 17, wherein said plurality of selectors are coupled to  
2 the first and second flip-flops of the shuffle unit in a topological manner that results  
3 in the first state value being output and the first and second flip-flops of the shuffle  
4 unit to store said second state value and a sixth data bit respectively when the  
5 corresponding one of said fourth plurality of data bits is in a first state, and the  
6 second state value being output and the first and second flip-flops of the shuffle unit  
7 to store the sixth data bit and said first state value respectively when the  
8 corresponding one of said fourth plurality of data bits is in a second state.

1 19. The apparatus of claim 18, wherein the shuffle units are serially coupled to  
2 each other with a first of the shuffle unit serially coupled to the first XOR gate, and  
3 said sixth data bit is a selected one of said second data bit and the output of an  
4 immediately preceding shuffle unit.

1 20. The apparatus of claim 14, wherein at least one of the shuffle units comprises  
2 a first and a second flip-flop to store a first and a second state value, and a plurality  
3 of selectors coupled to the first and second flip-flops to control modification of the  
4 first and second state values based on a corresponding one of said fourth plurality  
5 of data bits.

1 21. The apparatus of claim 20, wherein said plurality of selectors are coupled to  
2 the first and second flip-flops of the shuffle unit in a topological manner that results  
3 in the first and second flip-flops of the shuffle unit to store said second state value  
4 and a sixth data bit respectively when the corresponding one of said fourth plurality  
5 of data bits is in a first state, and the first and second flip-flops of the shuffle unit to  
6 store the sixth data bit and said first state value respectively when the corresponding  
7 one of said fourth plurality of data bits is in a second state.

1 22. The apparatus of claim 21, wherein the shuffle units are serially coupled to  
2 each other with a first of the shuffle unit serially coupled to the first XOR gate, and  
3 said sixth data bit is a selected one of said second data bit and the output of an  
4 immediately preceding shuffle unit.

1 23. The apparatus of claim 14, wherein the apparatus further comprises a  
2 register coupled to the second exclusive-OR gate to store a value to be periodically  
3 modified using the result of said combination of the fifth plurality of data bits.

1 24. The apparatus of claim 23, wherein the apparatus further comprises a  
2 function block coupled to the register to successively transform a modified version of

3 the stored value, and a mapping block coupled to register to generate a pseudo  
4 random bit sequence based on the successively transformed states of the modified  
5 value.

1 25. The apparatus of claim 14, wherein the apparatus is a stream cipher.

1 26. A method comprising:

2 generating a first, second and third plurality of data bits; and  
3 shuffling and propagating a fourth data bit generated from the first plurality of  
4 data bits, under the control of the second plurality of data bits, to output a fifth data  
5 bit to combine the third plurality of data bits.

1 27. The method of claim 26, wherein the fourth data bit is serially shuffle and  
2 propagated, and at each stage, a first state value is output when the corresponding  
3 one of said second plurality of data bits is in a first state, and a second state value is  
4 output when the corresponding one of said second plurality of data bits is in a  
5 second state.

1 28. The method of claim 26, wherein the fourth data bit is serially shuffle and  
2 propagated, and at each stage, a first of the state values is replaced by an input  
3 value, and shuffled, when the corresponding one of said second plurality of data bits  
4 is in a first state, and a second of the state values is replaced by the input value,  
5 and shuffled, when the corresponding one of said second plurality of data bits is in a  
6 second state.

ABSTRACT OF THE DISCLOSURE

A stream cipher is provided with one or more data bit generators to generate a first, second and third set of data bits. The stream cipher is further provided with a 5 combiner function having a network of shuffle units to combine the third set of data bits, using the first and second sets of data bits as first input data bits and control signals respectively of the network of shuffle units. In one embodiment, the shuffle units are binary shuffle units and they are serially coupled to one another.

100-00000000000000000000000000000000

## Dual Use Block/Stream Cipher

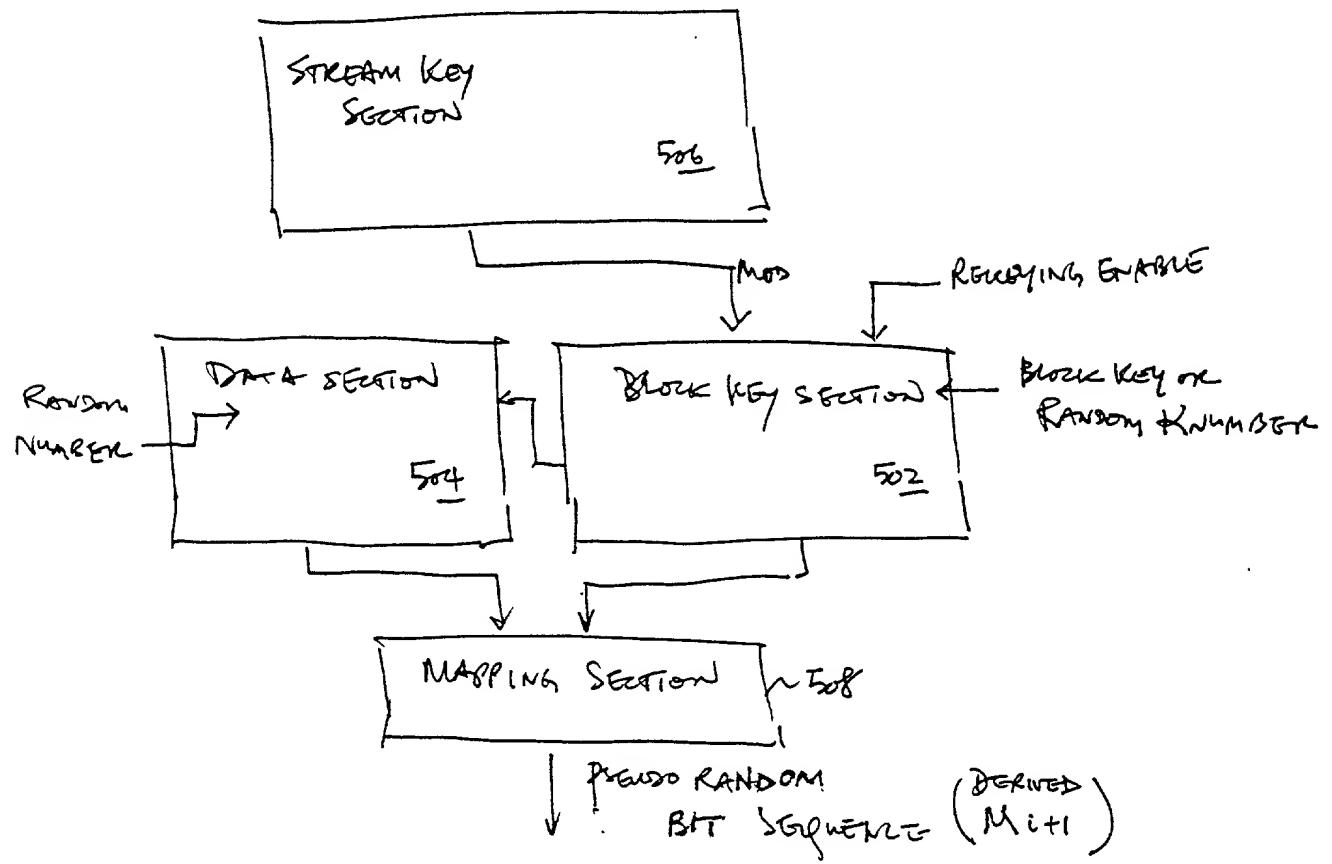


Fig. 1

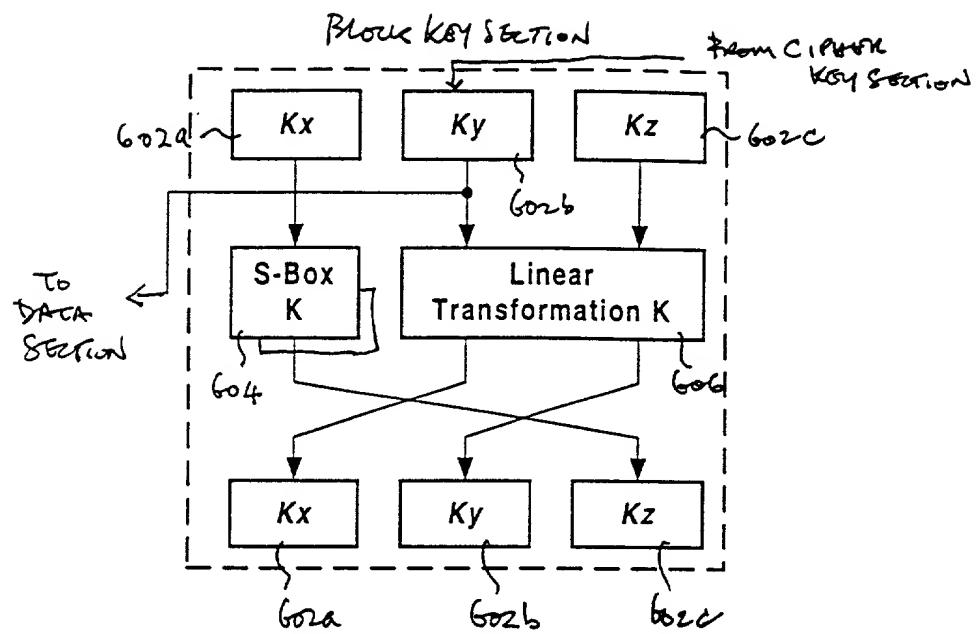


Fig. 2

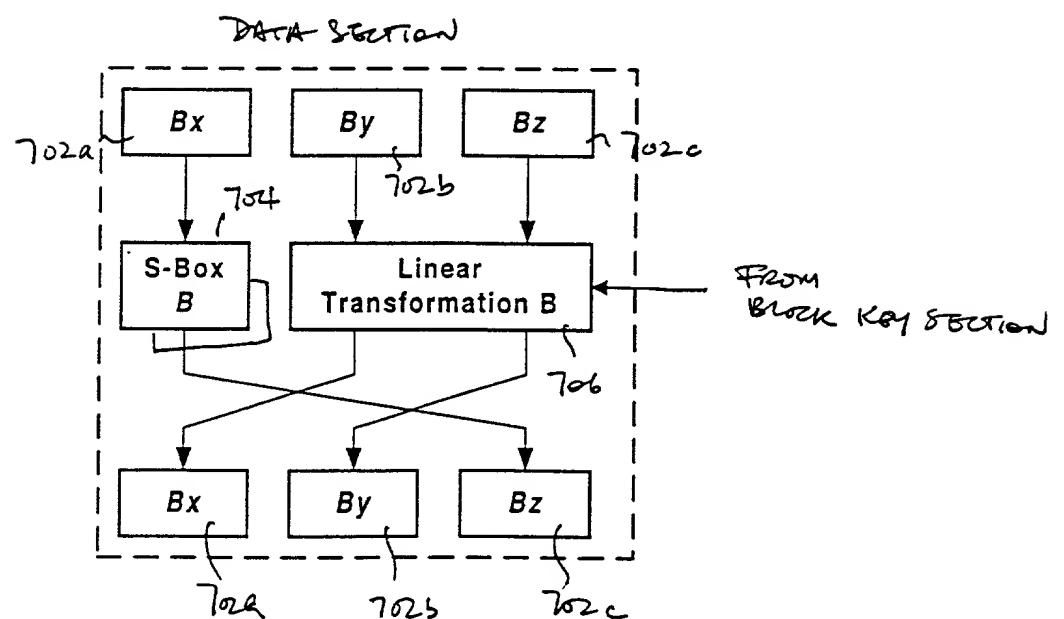


Fig. 3

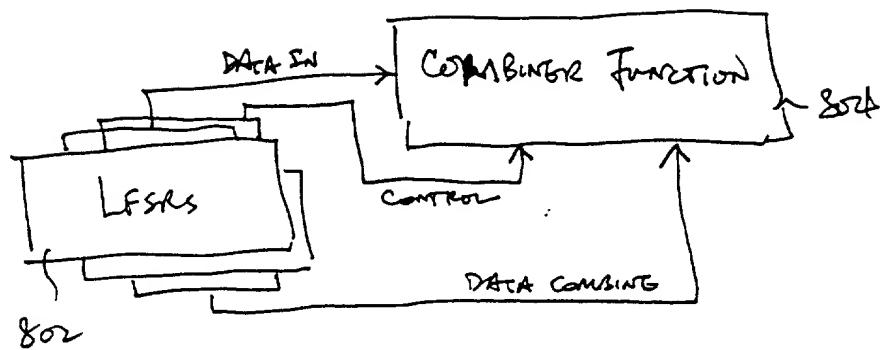


Fig. 4a

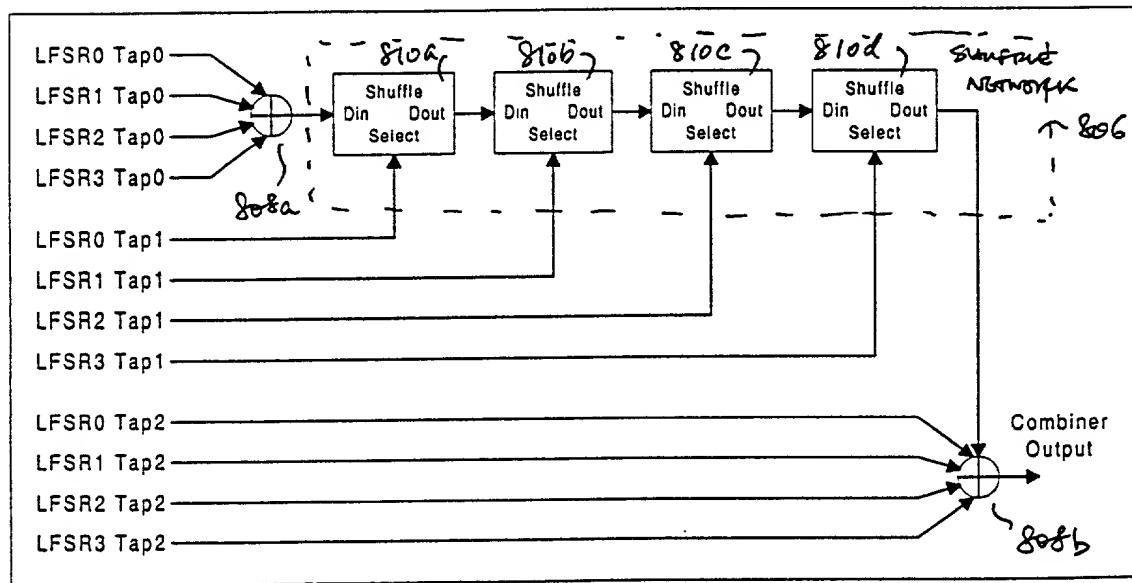


Fig. 4b

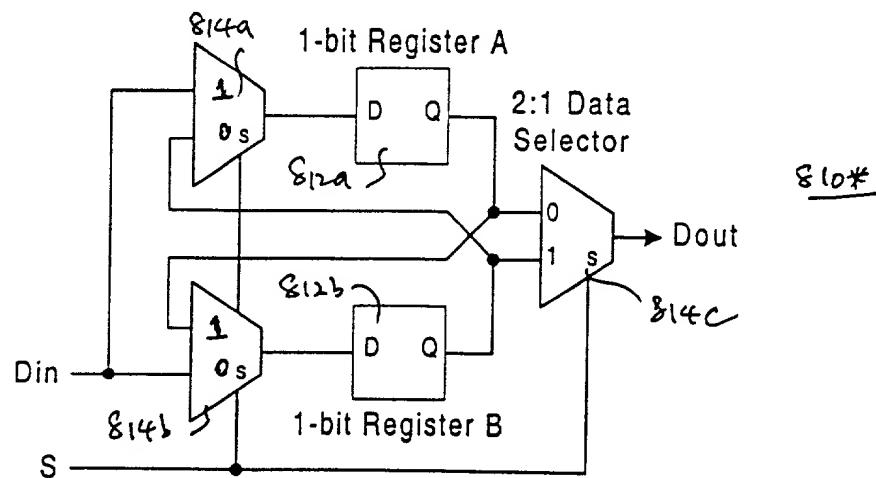


Fig. 4c

Attorney's Docket No.: 42390.P7574

PATENT

**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION**  
**(FOR INTEL CORPORATION PATENT APPLICATIONS)**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**A STREAM CIPHER HAVING A SHUFFLE NETWORK COMBINER FUNCTION**

the specification of which

XX is attached hereto.

— was filed on \_\_\_\_\_ as

United States Application Number \_\_\_\_\_

or PCT International Application Number \_\_\_\_\_

and was amended on \_\_\_\_\_.

(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

<u>Prior Foreign Application(s)</u>			<u>Priority Claimed</u>
<u>(Number)</u>	<u>(Country)</u>	<u>(Day/Month/Year Filed)</u>	<u>Yes</u> <u>No</u>

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

<u>(Application Number)</u>	<u>Filing Date</u>

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

<u>(Application Number)</u>	<u>Filing Date</u>	<u>(Status -- patented, pending, abandoned)</u>

I hereby appoint Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; Amy M. Armstrong, Reg. No. 42,265; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Kent M. Chen, Reg. No. 39,630; Yong S. Choi, Reg. No. P43,324; Thomas M. Coester, Reg. No. 39,637; Roland B. Cortes, Reg. No. 39,152; Barbara Bokanov Courtney, Reg. No. 42,442; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; Richard Leon Gregory, Jr., Reg. No. 42,607; Dinu Gruia, Reg. No. P42,996; David R. Halvorson, Reg. No. 33,395; Thomas A. Hassing, Reg. No. 36,159; Phuong-Quan Hoang, Reg. No. 41,839; Willmore F. Holbrow III, Reg. No. P41,845; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Thinh V. Nguyen, Reg. No. 42,034; Kimberley G. Nobles, Reg. No. 38,255; Babak Redjaian, Reg. No. 42,096; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Anand Sethuraman, Reg. No. P43,351; Charles E. Shemwell, Reg. No. 40,171; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; George G. C. Tseng, Reg. No. 41,355; Lester J. Vincent, Reg. No. 31,460; John Patrick Ward, Reg. No. 40,216; Stephen Warhola, Reg. No. 43,237; Charles T. J. Weigell, Steven D. Yates, Reg. No. 42,242; Reg. No. 43,398; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my attorneys, and James A. Henry, Reg. No. 41,064; Daniel E. Ovanezian, Reg. No. 41,236; Glenn E. Von Tersch, Reg. No. 41,364; and Chad R. Walsh, Reg. No. 43,235; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Cynthia Thomas Faatz, Reg. No. 39,973; Sean Fitzgerald, Reg. No. 32,027; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Jeffrey S. Draeger, Reg. No. 41,000; Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells, Reg. No. P43,256; and Alexander Ulysses Witkowski, Reg. No. P43,280; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Aloysius T.C. AuYeung, BLAKELY, SOKOLOFF, TAYLOR  
(Name of Attorney or Agent)  
& ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025  
and direct telephone calls to Aloysius T.C. AuYeung, (503) 684-6200.  
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Full Name of Sole/First Inventor** Gary L. Graunke

Inventor's Signature Gary L. Graunke Date Aug 29, 1999

Residence Hillsboro, Oregon Citizenship USA  
(City, State) (Country)

Post Office Address 362 NE Hillwood Drive  
Hillsboro, Oregon 97124

**Full Name of Second/Joint Inventor** David A. Lee

Inventor's Signature DA Date Aug 27, 1999

Residence Beaverton, Oregon Citizenship USA  
(City, State) (Country)

Post Office Address 740 SW Willow Creek Drive  
Beaverton, Oregon 97006

**Full Name of Third/Joint Inventor** Robert W. Faber

Inventor's Signature Robert W. Faber Date 29 August 1999

Residence Hillsboro, Oregon Citizenship USA  
(City, State) (Country)

Post Office Address 942 NE Third Avenue  
Hillsboro, Oregon 97124